セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
A. 6 情報セキュリティのための組織		
例外措置	「A.6.1.2 情報セキュリティの調整」に「非順守の事項をどのように扱うかを調整する。」と定められているが、導入時の手順書作成時に決めきらない例外事項への対処について、その確認手順を明確化しない場合が多い。 情報セキュリティ対策基準の運用にあたり例外措置事項が発生し得るが、その場合の対応が明確になっていないため、極端な場合は担当者が勝手に対策基準から外れた行為を行うようになる。	情報セキュリティ対策基準を運用する上で、内部規程で規定されていない事態や順守が困難な事態等の例外が発生した場合の対処についての確認や許可を得る手順を明確にする。 例外的事項の運用のすべてを内部規程(規則)で網羅することは非現実的であり、情報セキュリティの導入及び導入後の例外運用にスピード重視をするなら、情報セキュリティ管理者にその判断と許可の権限を付与しておくことが現実的である。
新しい情報処理設備導入時のリスク評価	「A.6.1.4 情報処理設備の認可プロセス」で「経営陣による認可プロセスを定め、実施、・・・」とあるが、実施の手引で「a) 新しい設備は，その目的及び用途について，適切な利用部門の経営陣の承認を得る。また，すべての関連するセキュリティ方針及び要求事項を確実に満たすために，その情報システムセキュリティ環境の維持に責任をもつ管理者からも承認を得る。」とガイドされているように、経営陣の承認だけでなく、情報セキュリティに責任を持つ管理者による新たなリスクの有無確認を得ることが重要である。しかし、経営陣の承認手順だけしか定めない場合がある。	新しい情報処理設備であっても、特別なルールではなく、組織内の決裁ルートに従った承認を得ればよく、そのルートに経営陣が含まれているのであれば、その決裁ルートに、情報セキュリティ面から適切な判断ができる人を加えればよい。新しい情報処理設備導入にあたっては、導入による関係システムへ及ぼす影響を含めて、新しい情報処理設備に関するリスクをあらかじめ評価し、さらに決済ルートのなかで情報セキュリティ面の問題がないかについて合議を得て、その後経営陣に承認を得る。
規制当局への報告	「A.6.1.6 関係当局との連絡」で、「関係当局との適切な連絡体制を維持しなければならない。」とあるが、実施の手引でガイドされている「脱法行為が疑われる場合の規制当局への報告手順」が、定められない場合がある。	脱法行為またはその恐れが検出された場合に、すみやかに規制当局(例えば、法の執行機関、監督官庁)に報告するための、責任と手順を備える。 例:個人情報漏えい時の管掌省庁への報告が遅れたり忘れたりしないように、事前に報告先や報告のための手順を明確にしておく必要がある。 また、外部への情報開示の観点から、一部の例外(事故の拡散、類似事案の発生)を除けば、マスコミなどを通じて、適宜、開示する。
情報セキュリティ専門団体との適切なコミュニケーション	「A.6.1.7 専門組織との連絡」で、「情報セキュリティの専門家による協会・団体との適切な連絡体制を維持・・・」とあるが、独立行政法人情報処理推進機構(IPA)、有限責任中間法人JPCERTコーディネーションセンター、などからの最新情報の収集や被害事例の届け出などの手順を確立していない場合がある。	情報セキュリティの専門の団体として、独立行政法人情報処理推進機構(IPA)、有限責任中間法人JPCERTコーディネーションセンター、及び他の協会・団体などからの情報セキュリティの最新情報の収集手順及びウイルス被害の発生等の事例の届け出手順を確立する。
Webサイト利用顧客の義務	「A.6.2.2 顧客対応におけるセキュリティ」で、「顧客に組織の情報又は資産へのアクセスを許す前に，明確にしたすべてのセキュリティ要求事項を満たすように対処・・・」とあるが、顧客が当方の事業所に来所した場合の情報資産へのアクセスにしか考慮されない場合がある。 A.6.2.2の実施の手引「 d) 次の事項を含むアクセス制御方針 1) 承認されたアクセス方法，並びに固有の識別子(例えば，利用者ID とパスワードとの組合せ)の管理及び使用 2) 利用者のアクセス及び特権の認可プロセス 3) 明示的に認可されていないすべてのアクセスを禁止することの表明 4) アクセス権を失効させる，又はシステム間の接続を阻止する手続」でガイドされているが、Webサイト会員などによるネットワーク経由での利用者に対する義務の取り決めも明確に示さなければならない。	Webサイト会員などの利用顧客には、Webサイトのアクセス権を与える前に、Webサイトの利用や貸与する会員IDやパスワード対する義務を、明示し、同意を得る。 また、法人の顧客に対して自組織のシステムに直接アクセスを許可する場合には、リスクを下げるために、顧客に対して許可するIPアドレスを制限するなどの要求事項を決め、同意を得る。

セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
再委託先の管理	「A.6.2.3 第三者との契約におけるセキュリティ」で「第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げ・・・」とあるが、再委託に関する要求、取り決めが十分でない場合がある。	委託契約については、組織の資産の保護に必要な再委託の制限を含める。委託先に再委託を許可する場合は、委託先に対する監督責任をどのように果たすのか、再委託先にある組織の資産の管理状況をどのように把握するのか、について責任と手順を明確にして、契約に含める。 経済産業省の個人情報保護法についてのガイドラインでは、受託者に必要かつ適切な監督を行っていない場合として「事例3）再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合」が示されている。
A. 7 資産の管理		
個人情報の特定とリスク認識	「A.15.1.4個人データ及び個人情報の保護」で関連法令の遵守が求められているが、特に個人情報の取扱いに関する法令等の遵守事項を考慮することが必要である。 個人情報保護マネジメントシステムに関するガイドラインでは、個人情報のライフサイクルに応じたリスクの評価と対応が求められている。	個人情報の取扱いについて受け取りから廃棄までのライフサイクルを明確にする。個人情報のライフサイクルごとに取扱責任者を明確にする。ライフサイクル上の個人情報の取り扱いの各局面ごとのリスク評価と対応策を明確にする。 これは、個人情報に限定した対応ではなく、重要な情報全般に対してこの手順で対応すべきで、とりわけ個人情報にはこの対応が必須である。
	情報セキュリティのリスクアセスメントの一般的な手法と、個人情報のリスクアセスメントで推奨されている手法に違いがある。 情報セキュリティでは、情報の保管場所におけるセキュリティ面の管理策だけが採用されるので、プライバシーマークを取得している場合のリスク認識と対策及び採用される対策内容が異なり、その結果、ルールの混在、誤解が生じやすい。	個人情報保護法だけでなく、JISQ15001、個人情報保護に関する省庁・自治体ガイドライン等も考慮して、個人情報取り扱いの各局面ごとに、個人情報に関する個人の権利対応(利用目的の通知、利用・提供の制限等)と安全保護(漏えい防止、利用者の限定、アクセス制限、入退室管理、確実な廃棄、等)について、適切な取扱い方法を定める。
顧客所有物	「A.7.1.1資産目録」で「すべての資産を明確に識別し、・・・」とあるが、これを当組織所有の資産と誤解して、顧客等から預かった資産やレンタル／リース品を含めないケースが見受けられる。	顧客等から預かった資産やレンタル／リース品は、当組織に管理責任があり、かつ契約等で善管注意義務の他に機密保護義務を締結している場合も多いので、セキュリティ上重要な資産として資産目録の対象にする。 メールに添付されて届く情報では、該当業務関係者以外の従業員にまで送付・転送されることもありえるので、注意が必要である。契約内容にもよるが、閲覧権限の範囲を管理しなければならない場合、メーリングリスト利用は避けるべきである。預かる情報については、改変の権限有無や開示条件などの確認も必要である。
法令･規制及び契約に伴う要求の特定	資産の機密性・完全性・可用性を評価する場合に、法令･規制及び契約に伴う要求を考慮すべきとされているが、資産ごとに「法令･規制及び契約に伴う要求」を特定していない場合がある。	資産ごとに「法令･規制及び契約に伴う要求」を特定し、機密性・完全性・可用性等の評価の参考にする。 例えば、個人情報保護法で保護される個人情報・個人データ・保有個人データ、会社法・税法・労働基準法等で保存が義務付けられる書類、顧客との契約で特別な対応が要求される情報、リース契約に基づく機器、著作権で保護されるソフトウェア／コンテンツ、などは該当する法令要求への対応が求められる。

セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
保管期間	資産の適正管理として適正な保管期間を定めて保管することが求められているが、保管期間を定めていない場合がある。	資産の適正管理のために、資産ごとに適正な保管期間を定める。 時間の経過とともに、機密性が薄れるなど機密性レベルが変化していくケースもあり、保管期間中の管理方法や保管期間満了時の廃棄方法の選択にも留意する。例えば、「プレスリリースまで秘密」のようなラベル表示をするとわかりやすい。
分類とラベル付け	「A.7.2.2情報のラベル付け及び取扱い」で定めた情報のラベル付け手順で「分類対象としない情報、ラベル貼付対象外とする情報」の定めがある場合、判断した上で分類・ラベル貼付けされていないのか、未判断で放置された情報かが区別できない。	すべての情報へのラベル貼付を義務づけるのが良いが、実施のハードルは高い。「貼付していない情報は、すべて公開情報として扱う」と定めるのも一方法である。しかし、この場合には、情報の分類とラベル貼付の判断から漏れた秘密情報がラベルなしのまま放置されるようでは困るので、これが防止ができるような手順とする必要がある。
A. 8　人的資源のセキュリティ		
雇用の終了又は変更	「A.8.3.1 雇用終了又は変更に関する責任」に「雇用の終了時は、実施中のセキュリティ要求事項及び法的責任，雇用終了以降一定期間継続する秘密保持契約（A.6.1.5参照），及び，雇用条件（A.8.1.3 参照）に規定された責任、について伝達する。雇用終了後もなお有効な責任及び義務は，従業員，契約相手及び第三者の利用者の契約に含める。」と定められているが、雇用の終了又は変更の手続きで当事者の守秘義務を負わせていない場合がある。	雇用の終了及び変更後も守秘義務（許可なく自己で使用することや第三者への開示・漏えいの禁止）を負わせる。 退職願と同時に手続きするのが合理的である。ただし、手続を行うことなく突然辞めたりするケースもあるので、採用時に署名してもらう誓約書に在職中の守秘義務だけでなく退職・契約終了後の守秘義務も合わせて記載しておくことが必要である。
外部委託の発注	「A.8.1.1（人的資源のセキュリティについての）役割及び責任」、「A.8.1.2選考」、「A.8.1.3 雇用条件」で、「従業員、契約相手及び第三者の利用者のすべての候補者について・・・」となっているが、管理策の「雇用」という呼称から、外部委託先の選定・発注に関して従業者の限定・識別・就業条件等について考慮することが漏れやすい。	雇用に関する役割及び責任、選考、雇用条件の管理策では、職員、契約社員等の臨時員、パートタイマ、アルバイトとは分けて、外部委託の発注の管理方法を定める。 委託先の選定においては、委託する業務の当組織における管理レベル以上の情報セキュリティ管理レベルを満たす企業の中から選定しなければならない。 委託の実施にあたっては、「自組織と委託先との法人間の委託契約」と「委託先法人と委託先の従業員個人との間の守秘義務契約」の両方が担保されることを確認する。
外部委託先の監督	「A.8.2.1 経営陣の（監督）責任」、「A.8.2.2 情報セキュリティの意識向上・教育及び訓練」、「A.8.2.3 懲戒手続」で、「すべての従業員、契約相手及び第三者の利用者について・・・」となっているが、管理策の「教育」、「懲戒手続」という呼称から、外部委託先の指導・契約上に対応について考慮することが漏れやすい。	経営陣の（監督）責任、情報セキュリティの意識向上・教育及び訓練、懲戒手続の管理策では、職員、契約社員等の臨時員、パートタイマ、アルバイトとは分けて、委託先の指導・契約上の管理方法を定める。 特に、委託した業務については、委託先の作業管理責任者を通して、委託先における貸与情報の管理や従事者の管理について指示し、かつ定期的に管理状況についての報告を受けるようにしなければならない。

セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
外部委託の終了	「A.8.3.1雇用終了又は変更に関する責任」、「A.8.3.2資産の返却」、「A.8.3.3アクセス権の削除」で、「すべての従業員、契約相手及び第三者の利用者について・・・」となっているが、管理策の「雇用終了」という呼称から、外部委託の業務の終了や委託契約の終了時の対応について考慮することが漏れやすい。	雇用終了又は変更に関する責任、資産の返却、アクセス権の削除の管理策では、職員、契約社員等の臨時員、パートタイマ、アルバイトとは分けて、外部委託の業務の終了や委託契約の終了時の対応についての管理方法を定める。 特に、委託した業務については、委託先に貸与した情報資産や情報の返却やコピーを含む消去、及びそれを確認したことの責任者の証明書などの他に、従事していた従事者の一人ひとりについての貸与した情報のコピーを含む消去、及びそれを確認したことの署名、業務終了後の守秘義務の確認書への署名について、作業管理責任者を通して報告を受けて確認しなければならない。
A. 9　物理的及び環境的セキュリティ		
オフィスのセキュリティ	「A.9.1.3 オフィス、部屋及び施設のセキュリティ」の実施の手引で「関連する安全衛生の規則及び標準を考慮する。」がガイドされているが、これが採用されない場合があり、装置の保守点検対応や置き場所により事故発生時の避難に影響を及ぼす可能性がある。	設備や情報機器の設置は、保守点検領域及び消防法に準拠した避難経路を考慮し、確保する。
外部での業務のセキュリティ	「A.9.2.1装置の設置及び保護」～「A.9.2.7資産の移動」は、資産が組織内に保管され、持ち出すことを例外として管理方法が例示されている。そのため、専ら外部で行う業務がありながら、その対応策が明確になっていない場合がある。	専ら外部で業務（建設工事、機器設置工事、使用量調査、料金徴収、宅配など）を行う場合の携行資産の安全保護のための管理方法を定める。
撮影録音機器・記録媒体等の持込	「A.9.2装置のセキュリティ」では、資産である装置の管理方法が例示されているが、組織内の情報を撮影録音又は複写しても持ち出す等によってセキュリティを脅かす個人的な装置の持ち込みによるリスクへの対応が定められていない場合がある。	撮影録音機器・記録媒体等の持込禁止や必要な場合の申請・許可のルールを定める。組織内の機密情報だけでなく、来客や業務委託の人が被写体になるリスクも考慮する。
A. 10　通信及び運用管理		
第三者提供サービスに関する受け入れテストの実施	「A.10.2.1第三者が提供するサービス」の実施の手引で「移行期間を通してセキュリティの維持を確実にする。」とガイドされているが、第三者提供サービスの運用開始前の稼働確認を「A.10.3.2システムの受け入れ」に沿って定めていない場合がある。	「A.10.3.2システムの受け入れ」に沿って、第三者提供サービスの運用開始前の稼働確認も行うように定める。
無線LAN及びモバイルネットワークのセキュリティ	「A.10.6.1 ネットワーク管理策」の実施の手引で「公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため，並びにネットワークを介して接続したシステム及び業務用ソフトウェアを保護するために，特別な管理策を確立する（A.11.4 及びA.12.3 参照）。」、及び「A.11.4.2 外部から接続する利用者の認証」の実施の手引で「無線ネットワークへのアクセスを管理するために，認証管理策を追加して実施することが望ましい。特に，無線ネットワークでは，ネットワークトラヒックの探知されない傍受及び挿入の機会が増大するので，管理策の選択には特別な注意が必要である。」とのガイドがされているが、無線LANやPHS、携帯などの無線ネットワークの管理策が適切に定められていない場合がある。	無線LAN及びモバイルネットワーク（PHS、携帯電話網など）を使用する場合は、無線ネットワーク特有のリスクを考慮したセキュリティ対応策を定める。特に、物理的な区画による対策が無線ネットワークに対しては保護効果がないことを考慮しなければならない。

セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
バックアップ媒体の保護	「A10.5.1 情報のバックアップ」の実施の手引で「バックアップ情報は，主事業所の災害による被害から免れるために，十分離れた場所に保管する。バックアップ情報に対して，主事業所に適用されている標準と整合した，適切なレベルの物理的及び環境的保護（A.9 参照）を実施する。主事業所で媒体に適用している管理策は，バックアップ情報の保管場所にも適用する。」とガイドされているが、これが採用されない場合がある。	災害の場合にでもバックアップから復旧に使えるように、バックアップはオリジナルと別場所に安全保護して保管するようにする。 バックアップの内容については、データ類だけでなく、ソフトウェアやドキュメント類についても、バックアップから復元できるようにしておく必要がある。 バックアップを輸送する場合、万一移送中に事故・事件に遭遇した場合であっても、内容のデータが漏えいしないように、暗号化またはその他の方法で保護する。
記録情報のバックアップ保存	バックアップが記録の保管目的をも兼ねている場合は、「A.15.1.3組織の記録の保護」に沿って法的な要求を考慮する必要があるが、法的対応としての「情報の保存期間」がバックアップ方針の中に盛り込まれていない場合がある。	バックアップが記録の保管目的をも兼ねている場合は、記録に対する法的な要求（A.15.1.3組織の記録の保護）等を考慮した管理手順を定める。 例えば、1年間の記録保管が要求されている場合、1年前の内容のバックアップが保存されるような、バックアップ媒体の世代管理・保管管理の方法としなければならない。 また、バックアップは改ざんのリスクへの考慮も必要である。例えば、1年間の記録保管が要求されるときに、ハードディスク上に1年以上記録できる容量のスペースを確保し、定期的にその全体をバックアップし、そのバックアップの最新1世代だけ保管するという運用を採用した場合、記録の改ざん発生後一度でもバックアップ作業を実行すると改ざん前の記録内容の復元ができなくなってしまうので、適切な方法とはいえない。
Webブラウザのセキュリティ設定	「A.10.4.2 モバイルコードに対する管理策」で、「認可されたモバイルコードが，明確に定められたセキュリティ方針に従って動作することを確実にする・・・」とあるが、要求事項が具体的でないために適切な対応が実施されていない。	Webブラウザでは、JAVAapplet、ActiveXコントロール、.NET Framework、その他のセキュリティレベルを、業務上必要でない限り、安全なレベルに設定するように定める。
電子メールの記録	「A.10.8.4電子的メッセージ通信」で、メール自体の保護だけではなく、デジタルフォレンジックの視点での対応が必要であるが、実施されていない場合がある。	電子メールは内部統制の検証、事件の証拠として重要なので、デジタルフォレンジックの視点からの対応として「A.13.2.3証拠の収集」にしたがって適切な記録保管を考慮する。
電子的取引オンライン取引利用時のセキュリティ	「A.10.9.1 電子商取引」、「A.10.9.2 オンライン取引」の実施の手引で、これら取引の場を提供する場合の取引の安全性確保についてガイドされているが、これらを利用する組織における利用上のセキュリティの対策がガイドされていない。	組織で、電子商取引やオンライン取引を利用する場合、これらの利用で誤りや不正が発生しないように、利用者の認定、利用の許可、他の者による利用結果の確認のための責任と手順を定める。
Webアクセス時のセキュリティ	Webブラウザによるホームページ やWebサイトのアクセスにおけるセキュリティへの対応が考慮されない場合がある。	Web アクセスを行う時のセキュリティ上の考慮事項を明確にする。 例えば、ウイルス対策、スパイウェア対策、フィッシング対策、ワンクリックによる料金請求の防止、ファイル交換ソフト(Winny等)による情報漏えい防止策、アダルトサイト・画像等の共有サイトやその他有料サイトへのアクセス制限、許可のないソフトウェア等のダウンロードの禁止、掲示板等への投稿制限、個人的な取引きの禁止など。

セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
Web サイトで収集するデータのセキュリティ	「A.10.9.1電子商取引」で「公衆ネットワークを経由する電子商取引に含まれる情報」についてのセキュリティが示されているが、「取引」でなくてWeb サイトでデータの収集だけを行う場合についての対応が示されていない。また、「10.9.3公開情報」で、ホームページ／Webサイトで提供する情報の完全性の保護が定められているが、収集する情報の完全性については定められていない。	Webサイトで収集し蓄積されたデータの改ざん防止、漏えい防止などのセキュリティについての対応を定める。 IPAで警告しているように、Webシステムについて、SQLインジェクション、OSコマンドインジェクション、ディレクトリトラバーサル、セッションIDの盗用、クロスサイトスクリプティング、クロスサイトリクエスト・フォージェリ、HTTP ヘッダインジェクション、メールの第三者中継、アクセス制御や認可制御の欠落、などのぜい弱性を検査して取り除くようにする。
監視による不正行為への対処	「A.10.10 監視」は「認可されていない情報処理活動を検知するため。」という目的になっているが、「A.10.10.1 監査ログ取得」、「A.10.10.2 システム使用状況の監視」では、事後の調査や監査用としてログを採取することが中心となっていて、不正アクセスを検知した場合に即時に対処し、不正アクセスを制止するような対応策が行われない場合が多い。	ログは記録・保管し事後に点検することだけでなく、ログを常時監視し許可のないアクセス等を検出した時に制止などの対処が即時にできることが重要である。 機密性レベルが極めて高い情報資産へのアクセスは事前許可制にしておき、事前申請のないアクセスを検知した場合に即時にアカウントを削除する等の対処ができるように、リアルタイムにログを収集、解析し、アラートを発信するような仕組みが望ましい。 外部等からの不正アクセスに対しては、不正アクセスが多いIPアドレスからのアクセスを拒否するなどの対策も必要になる。
A．11　アクセス制御		
利用者アクセス管理	「A.11.2.1 利用者登録」の実施の手引で「必要のない利用者 ID 及びアカウントがないかの定期的な，点検，及び，削除又は停止（A.11.2.4 参照）。」とのガイドがされているが、「A.8.3.3 アクセス権の削除」の雇用の終了又は変更時アクセス権の変更が速やかに漏れなく行える仕組みが整備されていない場合がある。	アクセス権は人事異動、担当替え、退職等の時に速やかに登録解除・変更の対応ができるように、従業員の異動が漏れなく捕捉され、通知され、登録解除・変更できる手順を策定する。 これらを効率よく漏れなく行うためには、各人ごとのアクセス権限を把握できる仕組(システム)が必要である。
パスワードの利用	「A.11.2.3 利用者パスワードの管理」の実施の手引で「新規，更新又は仮のパスワードを発行する前に利用者の身元を確認する手順を確立する。」とのガイドがされているが、決済など取引を伴う重要な操作のときの第二認証キーについては触れていない。 ネット上で、クレジットカード決済をする場合、第二認証キーとして、セキュリティコードを要求しているケースがあるが、第二認証キーとして生年月日の入力を要求する場合も増え、その時の生年月日データは、第二認証キーとして使われる。 したがって、生年月日は単なる個人情報としての保護管理だけでは不十分である。	ネット上で、クレジットカード決済をする場合、第二認証キーとして、セキュリティコードを要求しているケースがあるが、決済で、認証に利用するデータについては、決済情報としての機密性レベルで保護する対策をしなければならない。 自組織が提供するサービスだけでなく、他組織のサービスで一般的に収集、管理しているデータ項目を、第二認証キーに利用する場合は、慎重に検討することが重要である。 例えば、既に第二認証キーとして使われている生年月日に対しては、自組織でも慎重な管理が必要となる。
持ち込み情報機器の接続制限	「A.11.4.1 ネットワークサービスの利用についての方針」で、個人的なパソコンなどの機器を持ち込んでネットワークに接続することへの対応が明確に示されていない。また、「A.6.1.4情報処理設備の認可プロセス」の実施の手引で、個人・私的な情報処理設備の接続を組織が管理することについてガイドされているが、従業員や顧客が持ち込んだものを勝手にネットワークに接続することを技術的に排除することは示されていない。	従業員や顧客が持ち込んだパソコンなどの機器をネットワークへ接続することを技術的に抑止するための管理方法を定める。 ネットワーク認証を行う必要があり、MACアドレス制御が現実的である。

セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
A. 13 情報セキュリティインシデントの管理		
ヒヤリハットの報告	「A13.1.1情報セキュリティ事象の報告」、「A.13.1.2 セキュリティ弱点の報告」で情報セキュリティ事象の報告の定めがあるが、自分で体験した「ヒヤリハット」の報告が示されてない。	体験した「ヒヤリハット」を報告の対象として定める。情報セキュリティの事故を引き起こす現象を見つけたときにそれを報告し、事故の未然防止に生かすのは当然であるが、紛失や誤配送などの多くはヒューマンエラーを原因としているので、自分が失敗しそうになったときに、それを報告し、組織としてのヒューマンエラー防止策を検討し、事故の未然防止に役立てる。
情報セキュリティ事象による情報セキュリティインシデント防止	「A13.1.1情報セキュリティ事象の報告」、「A.13.1.2 セキュリティ弱点の報告」で情報セキュリティ事象を報告すべきことが示されているが、それを情報セキュリティインシデントの未然防止に活用することが明確に示されていない。	情報セキュリティ事象で報告されたことを情報セキュリティインシデントの未然防止に活用するための手順を定め実施する。 ハインリッヒの法則（1:29:300）から、日常の些細な300の事象を適切に予防に活かしてしていくことが重要である。 再発防止と共に予防処置が日常的に行われ、是正処置・予防処置の仕組み(システム化)が有効に働くように、方法・責任を明確にしておく。
A. 14 事業継続管理		
事業継続管理における業務中断のアセスメント	「A.14.1.2事業継続及びリスクアセスメント」の実施の手引で「業務プロセス中断の発生確率及び影響を，時間，損傷規模及び回復期間の面から判断するために，リスクアセスメントを行う。」とガイドされていて、情報システムの停止等が発生したときのシステム利用者や更にその先の顧客等への影響をアセスメントし、適切な復旧手順（事業継続計画）を決めるように示されている。 しかし、情報システムの停止等が発生したときのシステム利用者や更にその先の顧客等に対する影響のアセスメントを実施していない場合がある。（ときには、「情報資産のリスクアセスメント結果を参照」で済ませている場合があるが、情報資産のリスクアセスメントはリスクを低減し事故発生を未然防止するための管理策を選択・採用するためにアセスメントしたものである。事業継続管理においては、災害・事故等で情報システム停止等が起こってしまった後の復旧の緊急度・優先度を決めるために、情報システム停止等がどのように影響するかをアセスメントするものである。）	事業継続管理におけるリスクアセスメントでは、災害・事故等で情報システム停止等が発生してしまった時のサービス利用者への影響及びさらにその先の顧客など利害関係者への影響をアセスメントする。その影響の大きさに応じて、復旧の緊急度・優先順位、復旧の目標時間を定め、それに見合う復旧手順（事業継続計画）を策定する。 国民の生活のインフラ提供に影響する場合、又は社会への影響や自組織の経営上の影響が大きい場合は、復旧の優先度を上げ、復旧の目標時間の短縮を図るように、復旧のための復旧手順（事業継続計画）を決めて実装する。短時間で情報システムの復旧を行えるようにするには、離れた場所にある情報システムに速やかに切り替えて、情報システムを継続運用できるようなディザスタリカバリ対策が必要になる。
疾病等による人的資源の不足対策	「A.14.1.2 事業継続及びリスクアセスメント」の実施の手引で「例えば，装置の故障，人による誤り，盗難，火災，自然災害，テロ行為）の特定に基づく。」とガイドされており、ここで例示されていないが、国及び全世界における緊急的な政策になっている新型インフルエンザのような脅威が発生したときについて、広範囲な要員不足による可用性の維持について言及されていない。	新型インフルエンザなどの疫病の流行による業務中断の影響をアセスメントして対応方針を決める。従業員保護と事業要員確保のために、要員計画作成や通信手段整備、物資備蓄を行い、教育訓練を通じて周知・徹底して、有効な事業継続計画とする。

セキュリティ管理策作成のヒントとアドバイス

項　目	管理策作成上の課題	ヒントとアドバイス
A. 15 順守		
セキュリティツールの検証	「A.15.2.2技術的順守の点検」で技術的順守の点検が定められているが、実装した機器、ソフトウェア（ファイアウォール、ログ監視ソフト、バックアップツール等）が意図したとおりに機能しているかどうかを検証する手順等を定めていない場合がある。	セキュリティに関わる機器、ソフトウェアが適切に稼働しているかどうかを定期的に確認する手順を作成する。 この手順では、情報セキュリティ向上のために、機器、ソフトウェア（ファイアウォール、ログ監視ソフト、バックアップツール等）が意図したとおりに機能しているかどうか技術的な検証を行う。
監査における情報閲覧の制約への考慮	「A.15.3.1 情報システムの監査に対する管理策」で、監査活動による情報システムへのアクセスで情報の誤更新など業務への影響リスクを抑えるために、事前に監査人と慎重に監査方法を調整することが定められている。しかし、これら監査での監査人による情報の閲覧に関して、法令や契約で要求された守秘義務への違反に注意しなければならない。組織はISOや内部統制上から種々の内部監査を実施したり、また外部監査（第二者監査、第三者監査・審査）を受けるが、これらの監査における対応時の配慮事項の定めが十分でない場合がある。	内部監査、外部監査（第二者監査、第三者監査・審査）時の情報の閲覧に関して、法令や契約で要求された守秘義務への違反の防止についての対応策を定める。